

PROHIBITED ACTIVITIES

0915

(No. 20 September 2006)

IT Resource users may not knowingly and/or willingly utilize IT resources to:

- Transmit or access fraudulent, defamatory, harassing, obscene, or threatening information or for any communications prohibited by law; it is prohibited to:
 - Use obscene, profane, lewd, vulgar, inflammatory, threatening, or disrespectful language;
 - Engage in personal attacks, including prejudicial or discriminatory attacks;
 - View or print sexually explicit material;
 - Harass another person (for more information please refer to the 1000 Personnel Handbook Section 1086 at: <http://calfireweb/library/handbooks/1000/1086.pdf>);
 - Access, download, transmit, install or store discriminatory or offensive content (refer to Personnel Handbook Section 1400, Equal Employment Opportunity);
 - Post or transmit false or defamatory information about a person or organization (for further information regarding inappropriate information refer to the 1000 Personnel Handbook, §1086 Assaults, Threats, and Violence against Employees. <http://calfireweb/library/handbooks/1000/1086.pdf>);
- Engage in activities for partisan political campaigns or political fund raising;
- Engage in activities for personal gain, e.g. receiving money or other goods or services as a result of soliciting, promoting, selling, marketing or advertising products or services
- Access, download, transmit, install or store confidential information inappropriately;
- Access, download, transmit, install or store software that is not essential to job performance (examples include but are not limited to freeware or shareware, and music files);
- Access, download, transmit, install or store large files that are not essential to job performance;
- Read, alter, copy, or delete any other person's computer files without specific authorization from that person or his or her supervisor;
- Connect any computer, or network device to any of CAL FIRE's networks without prior approval by CAL FIRE's Chief Information Officer;
- Interfere with any other user's authorized access;
- Create, install, or distribute a computer virus, "Trojan horse," or other destructive program, or use key loggers or other spying/monitoring programs without prior authorization;
- Alter system software or hardware or circumvent control mechanisms without prior authorization;

- Copy or use software in violation of applicable copyrights or license agreements;
- Copy or share license keys, license data, or license codes without prior authorization;
- Engage in activities which compromise computer security or disrupt services, including using resources or accounts without authorization;
- Engage in activities to compromise or check for computer system or network security vulnerabilities without prior approval from the Chief Information Officer;
- Send electronic junk mail or chain letters;
- Encourage others to violate this policy.

[\(see next section\)](#)

[\(see HB Table of Contents\)](#)

[\(see Forms or Forms Samples\)](#)